



ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE:	Liaison Statement
TITLE:	Liaison Statement from ECMA TC 36 to ISO/IEC JTC 1/SC 27/WG 3
SOURCE:	ECMA Liaison Officer (H. Tabuchi)
DATE:	1999-09-30
PROJECT:	1.27.16
STATUS:	This document is being submitted for consideration at the next SC 27/WG 3 and SC 27 Plenary meetings in Columbia, MD, U.S.A., October 4 - 13, 1999.
ACTION:	ACT
DUE DATE:	1999-10-04
DISTRIBUTION:	P, O and L-Members W. Fumy, SC 27 Chairman M. De Soete, T. Humphreys, S. Knapskog, WG-Conveners H. Tabuchi, SC 27 Liaison Officer
MEDIUM:	Server
NO. OF PAGES:	3

TITLE: ECMA Liaison Statement to ISO/IEC JTC1/SC27/WG3
SOURCE: ECMA Liaison Officer, Haruki Tabuchi
DATE: 1999-9-27
PROJECT: JTC1.27.16
STATUS: For study by JTC1/SC27/WG3 experts

ECMA Liaison Statement
to ISO/IEC JTC1/SC27/WG3

Columbia, Maryland
1999-9-27

ECMA TC36 Liaison Reports to ISO/IEC JTC1/SC27/WG3

September 27, 1999

1. Nomination of ECMA as Protection Profile Registry

Mr. French, the chair man of TC36, reported about the nomination of ECMA as a PP Registry to the ECMA CC. Unfortunately the establishment of a PP-Registry by ECMA was not approved because of concerns on risks and benefit and because AFNOR has volunteered to develop such a registry. Consequently this work item will be dropped from the program of work for TC36.

We discussed the WD 15292 "Protection Profile registration procedures" from sponsors and users point of view. Following are our concerns and comments.

Clause 11.3 Defect notification

Concerns:

- A defect report turns out to be invalid but remains in the registry. It's not desirable as a public document.

Comments:

The process for retracting an erroneous defect report must be added. If the defect report is not valid and it's agreed, only a short history that a defect report was filed and retracted should be recorded.

Concerns:

- There is concern that a 'competitor' could write a defect report and if not answered in 30 days, the good PP could be marked obsolescent, which would not be good for the PP owner, for any vendor using the PP, or for any customer relying on the PP.

Comments:

There must be a way provided to reverse the automatic status change from obsolescent, with its accompanying reduction of review period, once a problem has been resolved.

2. E-COFC V2 and E-COFC/PP

A two-day Ad Hoc meeting was held on May 6 and 7. The objective of it was to update the E-COFC PP in correlation with the update of the E-COFC (version 2) and to finalize the documents. The participation of Gary Stoneburner and his expertise made it possible to achieve this goal. Main changes are the addition of a paragraph concerning the Usage of the INTERNET, a paragraph about Uniqueness of Origin, and the definition of Business Action.

This E_COFC version2 will be proposed to the ECMA CC as Update of the present E_COFC Standard ECMS 271.

At the same time Mr. Stoneburner gave as introduction a tutorial on "Using Common Criteria Protection Profiles". The viewgraphs are available as document ECMA/TC36/99/22. Hermann Siebert volunteered to do the final editing of the E-COFC PP documents.

Mr. U. Van Essen, BSI (German IT Security Agency) gave an overview of history and development of the Common Criteria and related activities, and answered questions concerning the present status, and involved organizations (Viewgraphs in ECMA/TC36/99/23). The MRA (Mutual Recognition Arrangement) within the EU concerning Security Evaluations, based on ITSEC, is in the process of extending to be based on the Common Criteria. The CCIMB (Common Criteria Interpretation Management Board, consisting of four European nations, Canada, NIST and NSA) is working with the European Commission towards an agreement on mutual recognition of the Common Criteria within the EU member states. The CEMEB (Common Evaluation Methodology Editorial Board) has completed the first version of the CEM (Common Evaluation Methodology) with assurance level up to EAL4 as basis. Main difference to the ITSEM is the emphasis on cost and effectiveness.

He then gave a short assessment of the E-COFC PP Draft and made some recommendations for improvement. Generally he concluded that the draft is mature.

E-COFC Public Business class PP will be proposed to the ECMA CC to be published as an ECMA TR.

3. Suppliers' Declaration of Conformity for IT Security

Use of suppliers' declaration of conformity for IT security products is proposed. We are interested in this issue as ECMA activity. We believe it could be acceptable to the IT market.

4. Liaison reports

The Polish National Institute of Telecommunications introduced IT security standardization issues. The Common Criteria are requiring for the Data Protection Act and the Protection of Secret Information and they schedule to start developing it as a Polish standard.

Japan introduced activities of CC. Their main activities that are under way are translation of ISO-15408 for Japanese Industrial Standard and development of evaluation methods based on CEM.